1.) Äquivalenzrelationen

Aufgaben: 3

```
> restart;
```

Definition und Beispiele

Äquivalenzrelationen verallgemeinern Gleichheit. Es handelt sich um die Gleichheit unter einem gewissen Aspekt. Formal führt man diesen grundlegenden Begriff wie folgt ein:

MATH: Man nennt $R \subseteq M \times M$ eine **Relation** auf einer Menge M.
- R heißt **reflexiv**, falls gilt: $\forall\ m \in M: (m, m) \in R$.
- R heißt **symmetrisch**, falls gilt: $(m_1, m_2) \in R \Rightarrow (m_2, m_1) \in R$.
- R heißt **transitiv**, falls gilt: $(m_1, m_2) \in R \wedge (m_2, m_3) \in R \Rightarrow (m_1, m_3) \in R$.

Wir schreiben auch aRb anstatt $(a, b) \in R$.

MATH: Eine Relation R auf einer Menge M heißt **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist.

Offenbar ist $M \times M$ eine Äquivalenzrelation auf M: Je zwei Elemente sind äquivalent.

ÜBUNG [01]:

Sind folgende Relationen Äquivalenzrelationen auf den jeweiligen Mengen M_i?

1) $M_1 := \{1, 2, 3\}$

```
> { [1,1], [2,2], [3,3], [1,2], [2,1] };
```

$$\{[1, 1], [1, 2], [2, 1], [2, 2], [3, 3]\} \quad \textbf{(1.1.1)}$$

2) $M_2 := \{1, 2, 3\}$

```
> { [1,1], [2,2], [3,3], [1,2], [2,1], [2,3], [3,2] };
```

$$\{[1, 1], [1, 2], [2, 1], [2, 2], [2, 3], [3, 2], [3, 3]\} \quad \textbf{(1.1.2)}$$

3) $M_3 := \mathbb{N}$

$a, b \in \mathbb{N}, aRb \Leftrightarrow a \leq b.$

4) M eine beliebige Menge, $M_4 := \mathrm{Pot}(M)$, die Potenzmenge,

$a, b \subseteq M, aRb \Leftrightarrow a \subseteq b \vee b \subseteq a.$

```
>
```

Äquivalenzklassen

MATH: Sei M eine Menge. Eine Menge P von Teilmengen von M heißt **Partition**

von M, falls drei Eigenschaften erfüllt sind:

1) $M = \bigcup_{X \in P} X,$
(M ist die Vereinigung aller Mengen aus P oder jedes Element von M kommt als Element bei einer Klasse von P mindestens einmal vor.)

2) $X, Y \in P \Rightarrow (X \cap Y = \varnothing \vee X = Y)$
(Je zwei verschiedene Mengen aus P haben einen leeren Durchschnitt, sie sind (paarweise) **disjunkt**, wie man sagt, oder: Jedes Element von M kommt als Element einer Klasse von P höchstens einmal vor.)

3) $\varnothing \notin P$
(Die leere Menge ist kein Element von P.)

Die Bedingungen 1) und 2) zusammen schreibt man manchmal auch so:

$$M = \biguplus_{X \in P} X,$$

Ist M die disjunkte Vereinigung von zwei Teilmengen M_1, M_2, also

$$M = M_1 \uplus M_2,$$

so ist

$$R := (M_1 \times M_1) \cup (M_2 \times M_2)$$

eine Äquivalenzrelation auf M.

DENKANSTOSS: Warum?

MATH: Ist R eine Äquivalenzrelation auf M und $a \in M$, so heißt die Menge

$$R(a) := \{b \in M \mid aRb\}$$

die **Äquivalenzklasse** von a. Jedes Element einer Äquivalenzklasse heißt auch **Vertreter** seiner Klasse. Es gilt offenbar: $R(a) = R(b) \Leftrightarrow aRb$. Die **Menge der Äquivalenzklassen** bildet eine **Partition** von M. Diese Partition wird mit M/R oder in Worten **M modulo R** bezeichnet. Eine Teilmenge von M, die aus jeder Äquivalenzklasse genau einen Vertreter enthält und darüberhinaus keine weiteren Elemente, heißt ein **Vertretersystem** oder eine **Transversale von R**.

Hier ist ein Programm zur Bestimmung der Äquivalenzklasse eines Elementes:

```
> AeKla:=proc(n::nonnegint,R::set(list))
    return map(j->j[2],select(i->i[1]=n,R));
  end proc:
> AeKla(1,RP);
```

$$\{1, 2, 3\} \qquad \textbf{(1.2.1)}$$

```
> map(a->AeKla(a[1],RP),RP);
```

$$\{\{1, 2, 3\}, \{8, 9, 10\}, \{4, 5, 6, 7\}\} \qquad \textbf{(1.2.2)}$$

MATH: Wir halten die grundlegende Tatsache fest, dass Äquivalenzrelationen und Partitionen verschiedene Beschreibungen derselben Sache sind.
Hier ist nun noch ein weiteres fundamentales Beispiel einer Äquivalenzrelation: Die Bildgleichheit.

Ist $f: M \to N$ eine Abbildung, so heißen $a, b \in M$ **bildgleich**, wenn $f(a) = f(b)$ gilt. Dies ist offenbar eine Äquivalenzrelation. Die zugehörige Partition ist die **Partition der** (nichtleeren) **Fasern** von f. Hier ist ein Programm, welches diese Äquivalenzrelation herstellt:

```
> Bilglei:=proc(M::set, f::procedure)
    local S;
    map(a->op(map(b-> if f(a)=f(b) then [a,b] end if,M)),M);
  end proc:
```

```
> f:=x->x mod 5;
```

$$f := x \to x \bmod 5 \qquad \textbf{(1.2.3)}$$

```
> M:={$1..20};
```

$$M := \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\} \qquad \textbf{(1.2.4)}$$

```
> M5:=Bilglei(M,f);
```

$$M5 := \{[1, 1], [1, 6], [1, 11], [1, 16], [2, 2], [2, 7], [2, 12], [2, 17], [3, 3], [3, 8], [3, 13], [3, 18], [4, 4], [4, 9], [4, 14], [4, 19], [5, 5], [5, 10], [5, 15], [5, 20], [6, 1], [6, 6], [6, 11], [6, 16], [7, 2], [7, 7], [7, 12], [7, 17], [8, 3], [8, 8], [8, 13], [8, 18], [9, 4], [9, 9], [9, 14], [9, 19], [10, 5], [10, 10], [10, 15], [10, 20], [11, 1], [11, 6], [11, 11], [11, 16], [12, 2], [12, 7], [12, 12], [12, 17], [13, 3], [13, 8], [13, 13], [13, 18], [14, 4], [14, 9], [14, 14], [14, 19], [15, 5], [15, 10], [15, 15], [15, 20], [16, 1], [16, 6], [16, 11], [16, 16], [17, 2], [17, 7], [17, 12], [17, 17], [18, 3], [18, 8], [18, 13], [18, 18], [19, 4], [19, 9], [19, 14], [19, 19], [20, 5], [20, 10], [20, 15], [20, 20]\} \qquad \textbf{(1.2.5)}$$

```
> map(a->AeKla(a[1],M5),M5);
```

$$\{\{1, 6, 11, 16\}, \{2, 7, 12, 17\}, \{3, 8, 13, 18\}, \{4, 9, 14, 19\}, \{5, 10, 15, 20\}\} \qquad \textbf{(1.2.6)}$$

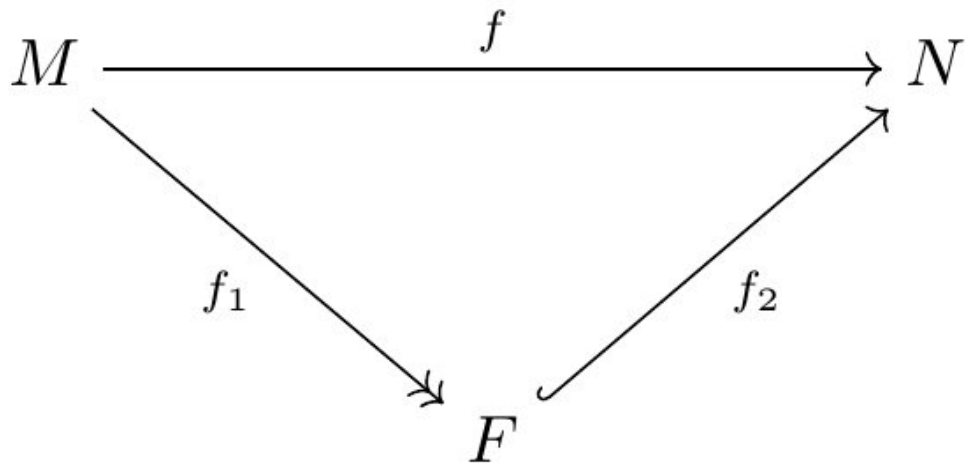
DENKANSTOSS: Wieviele Transversalen hat diese Äquivalenzrelation?

ÜBUNG [02]:

Sei m deine Matrikelnummer, $M := \{1,\ldots, m\}$ und $f: M \to \{0,\ldots, 41\} : a \mapsto a \bmod 42$. Wieviele Transversalen hat die Äquivalenzrelation der Fasern von f?

Zusammenhang: Abbildungen, Partitionen und Äquivalenzrelationen

Wenn du bislang alles verstanden hast, ist der nachfolgende sehr wichtige Satz sehr einfach einzusehen. Trotzdem ist er Ausdruck einer der erfolgreichsten Philosophien, an algebraische und kombinatorische Probleme heranzugehen.



MATH: ("Homomorphiesatz für Mengen") Sei $f: M \to N$ eine Abbildung. Dann gilt:
1) Die Menge
$F := \{ f^{-1}(\{n\}) \mid n \in \mathrm{Bild}(f) \}$
der nichtleeren Fasern von f bildet eine Partition von M mit zugehöriger Äquivalenzrelation "Bildgleichheit unter f".
2) Die Abbildung
$f_1 : M \to F : m \mapsto f^{-1}(\{f(m)\})$
ist eine surjektive Abbildung.
3) Die Abbildung
$f_2 : F \to N : f^{-1}(\{f(m)\}) \mapsto f(m)$
ist eine (wohldefinierte) injektive Abbildung.
4) Für die Komposition gilt
$f = f_2 \circ f_1$.

DENKANSTOSS: Gehe 1) bis 4) mit folgendem Beispiel durch:
M sei eine Menge von Briefen, die von Aachen aus verschickt werden sollen,
N sei eine Menge von Städten, so dass jede Stadt auf einer der Anschriften in M bei N vorkommt.
f sei die Abbildung, die jedem Brief seinem Bestimmungsort zuordnet.
Am Ende deiner Analyse solltest du eingesehen haben, dass es sich lohnt, die Briefe nach Städten zu ordnen, bevor man sie losschickt.

Wir haben bereits Programme, die alle vorkommenden Objekte konstruieren können.

```
> showstat(f);
```

```
f := proc(x)
   1   `mod`(x,5)
end proc
```

```
> M:={$3..20};
```

$$M := \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\} \quad \textbf{(1.3.1)}$$

```
> M5:=Bilglei(M,f);
```

$$M5 := \{[3, 3], [3, 8], [3, 13], [3, 18], [4, 4], [4, 9], [4, 14], [4, 19], [5, 5], [5, 10], [5, 15], [5, 20], [6, 6], [6, 11], [6, 16], [7, 7], [7, 12], [7, 17], [8, 3], [8, 8], [8, 13], [8, 18], [9, 4], [9, 9], [9, 14], [9, 19], [10, 5], [10, 10], [10, 15], [10, 20], [11, 6], [11, 11], [11, 16], [12, 7], [12, 12], [12, 17], [13, 3], [13, 8], [13, 13], [13, 18], [14, 4], [14, 9], [14, 14], [14, 19], [15, 5], [15, 10], [15, 15], [15, 20], [16, 6], [16, 11], [16, 16], [17, 7], [17, 12], [17, 17], [18, 3], [18, 8], [18, 13], [18, 18], [19, 4], [19, 9], [19, 14], [19, 19], [20, 5], [20, 10], [20, 15], [20, 20]\} \quad \textbf{(1.3.2)}$$

```
> F:=map(a->AeKla(a,M5),M);
```

$$F := \{\{6, 11, 16\}, \{7, 12, 17\}, \{3, 8, 13, 18\}, \{4, 9, 14, 19\}, \{5, 10, 15, 20\}\} \quad \textbf{(1.3.3)}$$

```
> f1:=map(a->op(map(S -> if a in S then [a,S] end if,F)),M);
```

$$f1 := \{[3, \{3, 8, 13, 18\}], [4, \{4, 9, 14, 19\}], [5, \{5, 10, 15, 20\}], [6, \{6, 11, 16\}], [7, \{7, 12, 17\}], [8, \{3, 8, 13, 18\}], [9, \{4, 9, 14, 19\}], [10, \{5, 10, 15, 20\}], [11, \{6, 11, 16\}], [12, \{7, 12, 17\}], [13, \{3, 8, 13, 18\}], [14, \{4, 9, 14, 19\}], [15, \{5, 10, 15, 20\}], [16, \{6, 11, 16\}], [17, \{7, 12, 17\}], [18, \{3, 8, 13, 18\}], [19, \{4, 9, 14, 19\}], [20, \{5, 10, 15, 20\}]\} \quad \textbf{(1.3.4)}$$

```
> f2:=map(A->[A,f(A[1])],F);
```

$$f2 := \{[\{6, 11, 16\}, 1], [\{7, 12, 17\}, 2], [\{3, 8, 13, 18\}, 3], [\{4, 9, 14, 19\}, 4], [\{5, 10, 15, 20\}, 0]\} \quad \textbf{(1.3.5)}$$

Wir lassen es als Übung, zu sehen, dass die Komposition von f_1 und f_2 gleich dem Folgenden ist:

```
> map(a->[a,f(a)],M);
```

$$\{[3, 3], [4, 4], [5, 0], [6, 1], [7, 2], [8, 3], [9, 4], [10, 0], [11, 1], [12, 2], [13, 3], [14, 4], [15, 0], [16, 1], [17, 2], [18, 3], [19, 4], [20, 0]\} \quad \textbf{(1.3.6)}$$

ÜBUNG [03]:

1) Verstehe die obigen Aussagen 1) bis 4) des Homomorphiesatzes und erkläre sie an dem obigen Beispiel mit **f** , **f 1** und **f 2**.
2) Insbesondere: was bedeutet "wohldefiniert" in 3)?
Hinweis: Was passiert, wenn $f^{-1}(\{f(m_1)\}) = f^{-1}(\{f(m_2)\})$ ist?
3) Sei M eine Menge. Begründe, dass Partitionen und Äquivalenzrelationen das selbe Konzept mit verschiedenen Sprachen beschreiben. Gebe dazu eine

(natürliche) Bijektion zwischen der Menge aller Partitionen von M und der Menge aller Äquivalenzrelationen auf M an.
Hinweis: Äquivalenzklassen.
4) Mach aus dem folgenden informellen Satz eine formelle mathematische Aussage und beweise diese:
"Jede Äquivalenzrelation (oder Partition) lässt sich als Bildgleichheitsrelation einer surjektiven Abbildung beschreiben."
Hinweis: Nutze die Abbildung, die ein Element auf seine Äquivalenzklasse schickt.
5) Rekonstruiere **f** aus **f 2** (als Menge von Paaren).

2.) Rekursion und Induktion: Rechnen mit natürlichen Zahlen

Aufgaben: 5

```
> restart;
```

Axiomatik der natürlichen Zahlen

Wir fangen noch einmal ganz von vorne an und stellen uns auf den Standpunkt, dass wir nur folgende Konzepte kennen:
1) Mengen
2) Abbildungen
Mit Hilfe dieser Konzepte und dem Prinzip der vollständigen Induktion wollen wir nun die natürlichen Zahlen konstruieren.

ACHTUNG: In den Aufgaben darf immer nur das verwendet werden, was weiter oben (in diesem Abschnitt) definiert oder bewiesen wurde, egal wie offensichtlich das Argument erscheint.

MATH: (**Peano-Axiome**) Will man verstehen, was die **natürlichen Zahlen** kennzeichnet, so ist es dieses:
1.) $\mathbb{N}$ ist eine Menge mit einer injektiven Abbildung
$\nu : \mathbb{N} \to \mathbb{N}$,
sodass das Komplement von $\mathrm{Bild}(\nu)$ in $\mathbb{N}$ aus genau einem Element besteht. Dieses nennen wir 1.
2.) Ist M eine Teilmenge von $\mathbb{N}$ mit den beiden Eigenschaften
a) $1 \in M$
b) $\nu(M) \subseteq M$,
so ist $M = \mathbb{N}$.

(Die Abbildung ν (griechisch: ***n***ü) nennt man ***N***achfolgerabbildung.)

MATH: ad 1.): Da endliche Mengen dadurch gekennzeichnet sind, dass injektive Selbstabbildungen bei ihnen schon bijektiv sind, impliziert 1.), dass $\mathbb{N}$ (falls es

existiert) bereits unendlich ist. Es hat sich nun eingebürgert, dass die Abbildung ν wie folgt geschrieben wird:

$$\nu : \mathbb{N} \to \mathbb{N} : r \mapsto r+1.$$

Von den Linksinversen von ν brauchen wir nur deren Einschränkung auf $\mathrm{Bild}(\nu)$. Diese ist dann natürlich eindeutig und wir bezeichnen sie mit

$$\pi : 1 + \mathbb{N} \to \mathbb{N} : r \mapsto r-1.$$

MATH: ad 2.) Dieses wird üblicherweise zweimal eingesetzt: Einmal bei Definitionen: Man spricht von Definition durch **Rekursion**. Zum anderen bei Beweisen: Man spricht von **vollständige**r **Induktion**.

Addition natürlicher Zahlen

BEISPIEL (Rekursion): Definition der **Addition** natürlicher Zahlen:
Für $a, b \in \mathbb{N}$ sei $a+b$ definiert durch:
a) Falls $b = 1$, dann sei $a + b := \nu(a)$.
b) Anderenfalls sei $a + b := \nu\big(a + \pi(b)\big)$.

Wir müssen uns davon überzeugen, dass dies eine widerspruchsfreie Definition ist, d.h. die rekursive Definition induziert eine Verknüpfung:

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

DENKANSTOSS: Dies ist genau dann der Fall, wenn für jedes $b \in \mathbb{N}$ die Abbildung

$$+_b : \mathbb{N} \to \mathbb{N}, a \mapsto a + b$$

wohldefiniert (siehe Def. Abbildung) ist.

Sei

$$M := \{b \in \mathbb{N} \mid a + b \text{ wohldefiniert für alle } a \in \mathbb{N}\}.$$

Mithilfe der Peano-Axiome verifizieren wir nun, dass $M = \mathbb{N}$ ist.
2a): $1 \in M$, wegen Teil a) der Definition: ν ist eine wohldefinierte Abbildung.
2b): Sei $b \in M$. Wir zeigen $\nu(b) \in M$.

$$a + \nu(b) = \nu\big(a + \pi(\nu(b))\big)$$ wegen Teil b) der Definition.

Weiter

$$\nu\big(a + \pi(\nu(b))\big) = \nu(a+b)$$ weil π linksinvers zu ν ist.

Insgesamt:

$$a + \nu(b) = \nu(a+b).$$

Also auch

$$\nu(b) \in M.$$

Praktisch sieht die Rekursion also so aus, dass wir π so oft wie möglich auf b anwenden, bis wir bei 1 sind, dann wenden wir ν auf a an, also Definition Teil a), und ν wieder genau so oft auf das jeweilige Ergebnis, wie wir π angewandt

haben, um b zu 1 zu reduzieren.

Wichtig: Wir sollten nichts über die neue Abbildung, die wir mit dem Symbol + notieren, annehmen, bevor wir es bewiesen haben. Insbesondere bedürfen Eigenschaften wie Assoziativität und Kommutativität eines Beweises.

BEISPIEL (vollständige Induktion): **Assoziativgesetz** für die Addition natürlicher Zahlen:
Behauptung: Für alle $a, b, c \in \mathbb{N}$ gilt:
$$(a+b)+c = a+(b+c).$$

Beweis durch Induktion.
Sei
$$M := \{c \in \mathbb{N} \mid (a+b)+c = a+(b+c) \ \forall\ a, b \in \mathbb{N}\}.$$

a) **Induktionsanfang** oder **Induktionsverankerung**:
$1 \in M$, denn
$(a+b)+1 = \nu(a+b)$ (Definition von ν)
$\nu(a+b) = a+\nu(b)$ (siehe Ende des Beweises der Wohldefiniertheit der Addition)
$a+\nu(b) = a+(b+1)$ (Defintion von ν)
Also
$(a+b)+1 = a+(b+1)$, d. h. $1 \in M$.

b) **Induktionsschritt** (Schluss von n auf $n+1$):
Sei $c \in M$. Wir müssen zeigen: $c+1 \in M$. Ersteres bedeutet
$(a+b)+c = a+(b+c) \ \forall\ a, b \in \mathbb{N}$.
Wir müssen also unter dieser Voraussetzung zeigen:
$(a+b)+(c+1) = a+(b+(c+1)) \ \forall\ a, b \in \mathbb{N}$.
Dies tun wir wie folgt:
$(a+b)+\nu(c) = \nu((a+b)+c)$ siehe Ende des Beweises der Wohldefiniertheit der Addition
$\nu((a+b)+c) = \nu(a+(b+c))$ siehe Induktionsvoraussetzung
$\nu(a+(b+c)) = a+\nu(b+c)$ siehe Ende des Beweises der Wohldefiniertheit der Addition
$a+\nu(b+c) = a+(b+\nu(c))$
siehe Ende des Beweises der Wohldefiniertheit der Addition
Insgesamt:
$(a+b)+\nu(c) = a+(b+\nu(c))$, d. h. $\nu(c) = c+1 \in M$.
Dies beendet unseren Induktionsbeweis.

MATH: Hier ist ein rekursives Programm, welches die Addition der natürlichen Zahlen auf der Basis der obigen Definition realisiert:

```
> ADDNAT:=proc(a::posint,b::posint)
    if b=1 then
      return a+1
```

```
    end if;
    ADDNAT(a,b-1)+1;
  end proc:
> ADDNAT(3,7);
                                10                              (2.2.1)
```

Um die Rekursion zu sehen:

```
> debug(ADDNAT):
  ADDNAT(3,7);
  undebug(ADDNAT):
{--> enter ADDNAT, args = 3, 7
{--> enter ADDNAT, args = 3, 6
{--> enter ADDNAT, args = 3, 5
{--> enter ADDNAT, args = 3, 4
{--> enter ADDNAT, args = 3, 3
{--> enter ADDNAT, args = 3, 2
{--> enter ADDNAT, args = 3, 1
<-- exit ADDNAT (now in ADDNAT) = 4}
                                5
<-- exit ADDNAT (now in ADDNAT) = 5}
                                6
<-- exit ADDNAT (now in ADDNAT) = 6}
                                7
<-- exit ADDNAT (now in ADDNAT) = 7}
                                8
<-- exit ADDNAT (now in ADDNAT) = 8}
                                9
<-- exit ADDNAT (now in ADDNAT) = 9}
                                10
<-- exit ADDNAT (now at top level) = 10}
                                10                              (2.2.2)
```

DENKANSTOSS: Wie oft ruft sich das Programm bei der Rechnung selbst auf? Warum ist es nicht ratsam, mit diesem Programm zu rechnen, wenn die Zahlen groß werden?

ÜBUNG [04]:

Beweise, dass die Addition natürlicher Zahlen kommutativ ist wie folgt:
Sei

$$M := \{b \in \mathbb{N} \mid a + b = b + a \ \forall\, a \in \mathbb{N}\}.$$

Zeige $M = \mathbb{N}$.
Hinweis: Die Induktionsverankerung ist wieder eine vollständige Induktion für sich.

Multiplikation natürlicher Zahlen

MATH: Rekursive Definition der Multiplikation natürlicher Zahlen:
Für $a, b \in \mathbb{N}$ sei $ab = a \cdot b$ definiert durch:
a) Falls $b = 1$, dann sei $a \cdot b := a$.
b) Anderenfalls sei $a \cdot b := a \cdot \pi(b) + a$.

DENKANSTOSS: Analog zum Fall der Addition ist sofort klar, dass diese Definition ohne Widerspruch ist.

MATH: Wir zeigen durch Induktion, dass das Distributivgesetz gilt:
$\forall\ a, b, c \in \mathbb{N}: (a+b) \cdot c = a \cdot c + b \cdot c$.

ANFANG INDUKTIONSBEWEIS:
Induktion nach c: $c = 1$ sofort aus der Defintion der Multiplikation (mit 1).
Angenommen $\forall\ a, b \in \mathbb{N}: (a+b) \cdot c = a \cdot c + b \cdot c$. Dann beweisen wir jetzt $(a+b) \cdot (c+1) = a \cdot (c+1) + b \cdot (c+1)$:
$(a+b) \cdot (c+1) = (a+b) \cdot c + (a+b)$ (Defintion der Multiplikation b) & π linksinvers zu ν)

$$(a+b) \cdot c + (a+b) = (a \cdot c + b \cdot c) + (a+b)$$

(Induktionsannahme)

$$(a \cdot c + b \cdot c) + (a+b) = (a \cdot c + a) + (b \cdot c + b)$$

(Assoziativ- und Kommutativgesetz der Add)

$(a \cdot c + a) + (b \cdot c + b) = a \cdot (c+1) + b \cdot (c+1)$ (Defin. Multiplikation b))
Also insgesamt
$(a+b) \cdot (c+1) = a \cdot (c+1) + b \cdot (c+1)$, was zu zeigen war.
ENDE INDUKTIONSBEWEIS

ÜBUNG [05]:

1) Schreibe analog zu dem obigen Programm **ADDNAT** ein Programm **MULNAT**, welches auf der Basis der rekursiven Definition der Multiplikation diese ausführt, wobei bei der Addition auf **ADDNAT** zurückgegriffen wird.
2) Wieviele **MULNAT**- und wieviele **ADDNAT**-Aufrufe erfordert **MULNAT(3,5)**?

ÜBUNG [06]:

1) Zeige $1 \cdot a = a\ \forall\ a \in \mathbb{N}$.
2) Unter Benutzung des Distributivgesetzes und Teil 1), zeige die Kommutativität der Multiplikation durch vollständige Induktion.
3) Unter Benutzung des Distributivgesetzes und Teil 2), zeige die Assoziativität der Multiplikation natürlicher Zahlen durch vollständige Induktion.
Hinweis: Das Distributivgesetz wurde oben nur einseitig bewiesen.

Division mit Rest

MATH: Auf $\mathbb{N}$ definieren wir eine Relation $<$ durch $a < b$ genau dann, wenn ein $c \in \mathbb{N}$ existiert mit $a + c = b$.

DENKANSTOSS: Folgere aus der Injektivität von ν, dass dieses c eindeutig bestimmt ist. (Induktion)

MATH: **Division mit Rest**: Sei $p \in \mathbb{N}$. Dann gibt es für jedes $n \in \mathbb{N}$ ein $q \in \mathbb{N}_0$, so dass entweder

$$n = q \cdot p$$

oder ein $r \in \mathbb{N}$ existiert mit $r < p$ und

$$n = q \cdot p + r.$$

Im ersten Fall heißt n durch p **teilbar**. Im zweiten Fall heißt r der **Rest** modulo p. In beiden Fällen heißt q der (ganzzahlig gemachte) **Quotient** von n und p.

BEISPIEL: $p = 11$:

```
> iquo(133,11);
  irem(133,11);
```

$$12$$

$$1 \qquad \textbf{(2.4.1)}$$

```
> 133 mod 11;
```

$$1 \qquad \textbf{(2.4.2)}$$

Oder auch in einem Befehl:

```
> iquo(133,11,'r');
  r ;
```

$$12$$

$$1 \qquad \textbf{(2.4.3)}$$

bzw.

```
> irem(133,11,'q');
  q;
```

$$1$$

$$12 \qquad \textbf{(2.4.4)}$$

p-adische Darstellung natürlicher Zahlen

Wir hatten oben bereits gesehen, dass das Rechnen streng nach den Definitionen (**ADDNAT**, **MULNAT**) zu aufwendig ist. Die p-adische Darstellung liefert einen besseren Weg.

MATH: (Entwicklung natürlicher Zahlen nach p-Potenzen) Sei $p \in \mathbb{N}$, $p > 1$. Dann lässt sich jede natürliche Zahl n nach Potenzen von p entwickeln, wobei die Koeffizienten zwischen 0 und $p - 1$ liegen (Null ist zwar keine natürliche Zahl, aber wenn 0 als Koeffizient auftritt, soll das einfach bedeuten, dass der

entsprechende Summand entfällt):

$$n = n_1 + n_2 \cdot p + n_3 \cdot p^2 + \ldots + n_k \cdot p^{k-1}$$

mit $n_k \neq 0$.

ÜBUNG [07]:

1) Schreibe ein rekursives Programm, welches für gegebene n, p die Entwicklungskoeffizienten n_i ausrechnet und als endliche Folge $[n_1, n_2, \ldots, n_k]$ ausgibt. Teste das Programm auch an einigen Beispielen.
2) Sei nun n deine Matrikelnummer: Wie sieht die Folge der Entwicklungskoeffizienten von n für $p = 10$ aus? Vergleiche dies mit der Ziffernfolge der Zahl.
3) Erläutere, warum mit der Kodierung natürlicher Zahlen durch ihre p-adische Darstellung das Problem der Addition und Multiplikation mit den Rekursionstiefen gelöst wird.
Hinweis: Denke an die schriftlichen Rechenverfahren aus der Grundschule.

Mit Hilfe einer p-adischen Darstellung können wir jetzt vergleichsweise bequem in ; addieren und multiplizieren, wie wir das bereits seit unserer Grundschulzeit (mit $p = 10$) tun.

MATH: Das Potenzieren hat immer noch ein gewisses Problem mit der Rekursionstiefe, wenn wir dieses ebenfalls naiv definieren würden. Dieses kann man aber ein gutes Stück weit entschärfen, wie folgendes Programm zeigt: Wir benutzen die 2-adische Darstellung des Exponenten um Potenzieren auf Quadrieren und gelegentliches Multiplizieren zurückzuführen. Dieses Verfahren wird oft als Square&Multiply bezeichnet:

```
> potnat:=proc(a::posint,b::posint)
    if b=1 then
      return a;
    end if;
    if irem(b,2)=0 then
      return potnat(a,b/2)^2;
    end if;
    return(potnat(a,b-1)*a);
  end proc:
> potnat(3,3);
  potnat(3,4);
  potnat(3,5);
                          27
                          81
                         243                          (2.5.1)
```

DENKANSTOSS: Verstehe das Programm **potnat**. Wie bestimmt die 2-adische Darstellung von b den Ablauf des Programms? Wie viele Quadrate und Produkte werden berechnet?